

## What is Claimed:

1           1. A method for performing modular division operations used in a  
2 cryptographic process over a finite field  $F_U$  defined for a prime number  $U$ , in which  
3 values are divided by an integer divisor  $V$  modulo  $U$ , the method comprising the steps  
4 of calculating an arithmetic inverse of  $V$  modulo  $U$  using an extended greatest  
5 common divisor (GCD) method which includes a plurality of reduction steps and a  
6 plurality of inverse calculations, including the steps of:

7           assigning  $U$  and  $V$  as initial values to respective temporary variables  $U3$   
8 and  $V3$  which are used to calculate the GCD of  $U$  and  $V$ ;

9           assigning initial values to respective temporary variables  $U2$  and  $V2$   
10 which are used to calculate an arithmetic inverse of  $V$  modulo  $U$ ;

11           testing a condition and, if the condition tests true,

12                 combining multiple ones of the plurality of reduction steps  
13 for calculating the GCD; and

14                 combining multiple ones of the plurality of inversion  
15 calculations; and

16           if the condition tests false,

17                 performing a single one of the reduction steps; and

18                 performing a single one of the inverse calculation steps.

1           2. A method according to claim 1, wherein:

2           the extended GCD algorithm is a binary GCD algorithm;

3           the step of testing the condition includes the step of determining if  $U3$   
4 has a number,  $N$ , of zero-valued least significant bits (LSBs), where  $N$  is an integer  
5 greater than one;

6           the step of combining multiple ones of the plurality of reduction steps  
7 includes shifting the value in  $U3$  by  $N$  bit positions to less significant bit positions;  
8 and

9           the step of combining multiple ones of the plurality of inversion  
10 calculations includes the steps of:

11 retrieving a value to be combined with V2 from a look-up table  
12 responsive to the value of N;

13 combining the retrieved value from V2 to obtain a combined  
14 value in V2; and

15 shifting the combined value in V2 by N bit positions to less  
16 significant bit positions.

1 3. A method according to claim 2, wherein the look-up table  
2 includes a plurality of multiples of U.

1 4. A method according to claim 3, wherein the step of retrieving the  
2 value to be combined with V2 from a look-up table includes the steps of:

3 indexing a first further look-up table responsive to two of the LSBs of  
4 V2 if N equals 2 to obtain an index value;

5 indexing a second further look-up table responsive to three of the LSBs  
6 of V2 if N is greater than 2 to obtain the index value; and

7 indexing the look-up table by the index value.

1 5. A method according to claim 1, wherein:  
2 the extended GCD algorithm is a left-shift binary GCD algorithm; and  
3 the steps of combining multiple ones of the plurality of reduction steps  
4 and combining multiple ones of the plurality of inversion calculations includes the step  
5 of performing a reduction step according to a Lehmer GCD method.

1 6. A method according to claim 5, wherein, the step of testing the  
2 condition includes the step of determining if a bit position of a most significant bit  
3 (MSB) of the value in U3 differs by less than a predetermined number from a bit  
4 position of an MSB of the value in V3.

1 7. A computer readable carrier including computer program  
2 instructions that cause a computer to perform modular division operations over a finite  
3 field  $F_U$  that defined for a prime number U and used in a cryptographic process in  
4 which values are divided by an integer divisor V modulo U, the method comprising  
5 the steps of calculating an arithmetic inverse of V modulo U using an extended

6 greatest common divisor (GCD) method which includes a plurality of reduction steps  
7 and a plurality of inverse calculations, including the steps of:

8 assigning U and V as initial values to respective temporary variables U3  
9 and V3 which are used to calculate the GCD of U and V;

10 assigning initial values to respective temporary variables U2 and V2  
11 which are used to calculate an arithmetic inverse of V modulo U;

12 testing a condition and, if the condition tests true,

13 combining multiple ones of the plurality of reduction steps  
14 for calculating the GCD; and

15 combining multiple ones of the plurality of inversion  
16 calculations; and

17 if the condition tests false,

18 performing a single one of the reduction steps; and

19 performing a single one of the inverse calculation steps.

1 8. A computer readable carrier according to claim 7, wherein the  
2 extended GCD algorithm is a binary GCD algorithm and the computer program  
3 instructions which implement the step of testing the condition cause the computer to  
4 perform the step of determining if U3 has a number, N, of zero-valued least  
5 significant bits (LSBs), where N is an integer greater than one;

6 the computer program instructions which implement the step of  
7 combining multiple ones of the plurality of reduction steps cause the computer to  
8 perform the step of shifting the value in U3 by N bit positions to less significant bit  
9 positions; and

10 the computer program instructions which implement the step of  
11 combining multiple ones of the plurality of inversion calculations cause the computer  
12 to perform the steps of:

13 retrieving a value to be combined with V2 from a look-up table  
14 responsive to the value of N;

15 combining the retrieved value from V2 to obtain a combined  
16 value in V2; and

17                   shifting the combined value in V2 by N bit positions to less  
18           significant bit positions.

1                   9.     A computer readable carrier according to claim 8, wherein the  
2     look-up table includes a plurality of multiples of U.

1                   10.    A computer readable carrier according to claim 9, wherein the  
2     computer program instructions that implement the step of retrieving the value to be  
3     combined with V2 from a look-up table cause the computer to perform the steps of:

4                   indexing a first further look-up table responsive to two of the LSBs of  
5     V2 if N equals 2 to obtain an index value;

6                   indexing a second further look-up table responsive to three of the LSBs  
7     of V2 if N is greater than 2 to obtain the index value; and

8                   indexing the look-up table by the index value.

1                   11.    A computer readable carrier according to claim 7, wherein the  
2     extended GCD algorithm is a left-shift binary GCD algorithm and the computer  
3     program instructions that cause the computer to perform the steps of combining  
4     multiple ones of the plurality of reduction steps and combining multiple ones of the  
5     plurality of inversion calculations includes the step of performing a reduction step  
6     according to a Lehmer GCD method.

1                   12.    A computer readable medium according to claim 11, wherein, the  
2     computer program instructions that implement the step of testing the condition cause  
3     the computer to perform a step of determining if a bit position of a most significant bit  
4     (MSB) of the value in U3 differs by less than a predetermined number from a bit  
5     position of a bit position of an MSB of the value in V3.

1                   13.    Cryptographic apparatus which performs division operations over  
2     a finite field  $F_U$  defined for a prime number U, in which values are divided by an  
3     integer divisor V modulo U, the apparatus calculating an arithmetic inverse of V  
4     modulo U using an extended greatest common divisor (GCD) algorithm which  
5     includes a plurality of reduction steps and a plurality of inverse calculations, the  
6     apparatus comprising:

7                   means for assigning U and V as initial values to respective temporary  
8     variables U3 and V3 which are used to calculate the GCD of U and V;

means for assigning initial values to respective temporary variables U2 and V2 which are used to calculate an arithmetic inverse of V modulo U;

means for testing a condition; and

means for combining multiple ones of the plurality of reduction steps and multiple ones of the inverse calculations if the condition test true;

14. Cryptographic apparatus according to claim 13, wherein:

the extended GCD algorithm is a binary GCD algorithm;

the means for testing the condition includes means for determining if U3 has a number, N, of zero-valued least significant bits (LSBs), where N is an integer greater than one;

the means for combining multiple ones of the plurality of reduction steps includes means for shifting the value in U3 by N bit positions to less significant bit positions; and

the means for combining multiple ones of the plurality of inversion calculations includes:

means for retrieving a value to be combined with V2 from a look-up table responsive to the value of N;

means for combining the retrieved value from V2 to obtain a combined value in V2; and

means for shifting the combined value in V2 by N bit positions to less significant bit positions.

15. Apparatus according to claim 14, wherein the look-up table includes a plurality of multiples of U.

16. Apparatus according to claim 15, wherein:

the means for retrieving the value to be combined with V2 from a look-up table includes:

means for indexing a first further look-up table responsive to two of the LSBs of V2 if N equals 2 to obtain an index value;

6 means for indexing a second further look-up table responsive to three of  
7 the LSBs of V2 if N is greater than 2 to obtain the index value; and

8 means for indexing the look-up table by the index value.

1 17. Apparatus according to claim 13, wherein:

2 the extended GCD algorithm is a left-shift binary GCD algorithm; and

3 the means for combining multiple ones of the plurality of reduction steps  
4 and multiple ones of the plurality of inversion calculations includes means for  
5 performing a reduction step according to a Lehmer GCD method.

1 18. Apparatus according to claim 17 wherein, the means for testing  
2 the condition includes means for determining if a bit position of a most significant bit  
3 (MSB) of the value in U3 differs by less than a predetermined number from a bit  
4 position of an MSB of the value in V3.